IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF OREGON

PORTLAND DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

KYLE SCOTT BROADHURST,

Defendant.

3:11-cr-00121-MO-1

OPINION AND ORDER

MOSMAN, J.,

On January 24, 2011, Clackamas County Deputy Sheriff Erin Schweitzer and Detective Ken Link used a handheld device on defendant Kyle Scott Broadhurst's property to monitor wireless radio signals. Based on the data they collected, they subsequently obtained a search warrant for defendant's residence. On February 16, 2011, officers executed the search warrant and collected incriminating evidence. Defendant now moves to suppress all evidence obtained as a result of the search warrant on two grounds. First, he argues any use of this device constitutes a search under the Fourth Amendment. Second, he argues Deputy Sheriff Schweitzer and Detective Link unlawfully searched his residence by trespass, all evidence collected was tainted by this unlawful search, and there is no independent source for admission of the otherwise

tainted evidence. I determine the use of the handheld device did not violate the Fourth Amendment. But I also find the warrant affidavit, once cleared of all information tainted by the trespass, fails to state probable cause. Therefore, I GRANT defendant's motion to suppress [39].

BACKGROUND

I. Preliminary Monitoring of Child Pornography File-Sharing

In May 2010, Deputy Sheriff Schweitzer was investigating the sharing of child pornography files over the Internet through peer-to-peer ("P2P") networks.[1] She traced the files

[1] Glossary of Terms:

Access Point: An access point is most commonly incorporated into a wireless router, which is hardwired to a network, and allows wireless devices to connect to that network. (Tr. [49] at 24:5–12.)

Globally Unique Identifier (GUID): A GUID is a random string of numbers and letters created when P2P software is installed on a computer. A GUID is unique to each computer. It is stored on the computer and can be seen by peers who download files from that computer. A GUID is the same for all files shared by the computer, even though each file has a unique SHA-1 value. Similar to an IP address that identifies a computer connected to the Internet, a GUID identifies a computer connected to a P2P network. (Schweitzer Aff. [42-1] at 6–8.)

Internet Protocol ("IP") Address: "An IP address is a standard way of identifying a [device] that is connected to the Internet. An IP address is comprised of four integers less than 256 separated by periods." *United States v. Heckenkamp*, 482 F.3d 1142, 1144 n.1 (9th Cir. 2007).

Media Access Control (MAC) Address: A MAC address is a unique code identifier assigned to a network communication device, such as a wireless router or laptop computer, by its manufacturer. (Schweitzer Aff. [42-1] at 18.)

P2P Network: A P2P network facilitates the sharing of files over the Internet. A computer user, or "peer," can install P2P software on a computer to access the P2P network. With P2P software, a peer can search for digital files, such as pictures, being shared on the network and select particular files to download. Once downloaded, the peer has a digital copy of the shared file on his computer. *See United States v. Flyer*, 633 F.3d 911, 913–14 (9th Cir. 2011); *United States v. Lynn*, 636 F.3d 1127, 1130 (9th Cir. 2011).

Secure Hash Algorithm Version 1 (SHA-1) Value: A SHA-1 value is best described as a digital fingerprint of a computer file. *See United States v. Glassgow*, 682 F.3d 1107, 1110 n.2 (8th Cir. 2012). A file's SHA-1 value will remain the same regardless of the file's location or name. However, modifying a file will change the SHA-1 value. When a peer searches for a file over a P2P network, the peer can view the file's SHA-1 value. (Schweitzer Aff. [42-1] at 6.)

Set Service Identifier ("SSID"): The SSID is the name of the access point or wireless network. For example, when a computer searches for wireless networks, the user will see the names of the networks, and those names are the SSIDs. (Tr. [49] at 26:14–24.)

back to a set of computers in the Linwood School neighborhood. With the police software Peer Spectre, Deputy Sheriff Schweitzer recorded the time and date of the file transmissions, and the SHA-1 value and filenames of the transmitted files. She also used her access to the P2P network, without additional software, to obtain the IP addresses of the computers sharing the child pornography files. Over the following eight months, Deputy Sheriff Schweitzer used Peer Spectre and the P2P network to identify ten IP addresses in the Linwood School neighborhood that were sharing thousands of child pornography files. (Schweitzer Aff. [42-1] at 14–16.)

II. Active Investigation of Linwood School Neighborhood

On September 22, 2010, Deputy Sheriff Schweitzer began an active investigation of these ten IP addresses. She obtained their subscriber information through internet service provider ("ISP") subpoenas. (*Id.* [42-1] at 13, 16–17.) This subscriber information revealed that the ten IP addresses were registered to six residences in the Linwood School neighborhood, including defendant's residence. Deputy Sheriff Schweitzer also determined that the Internet connections of these IP addresses were accessible through unsecured wireless networks. Based on this fact, Deputy Sheriff Schweitzer believed only one individual was accessing the unsecured wireless networks to share child pornography files. (*Id.* [42-1] at 16–18.)

It is important to note, however, that because these wireless networks were unsecured, any individual with a wireless capable device within signal range could have accessed them. Therefore, there was no reason to conclude that the individual sharing child pornography files

---

Station Device: Computers, tablets, smartphones, or any other wireless capable devices are typical examples of station devices. The user of a station device connects to an access point by requesting to join a network. (*Id.* [49] at 24:21–25:5.)

Received Signal Strength Indicator ("RSSI"): RSSI is a range of numbers between -60 to 6 that indicates the strength of a radio signal emitting from an access point or station device. (Ex. D at 23–24.)

did so from within one of the six previously identified residences. Indeed, that individual could have accessed these unsecured wireless networks just as easily from any other location within signal range. For example, he could have accessed them from any other nearby home, or even from a parked car using a laptop or other wireless capable device.

To find the location of the device accessing the unsecured networks, Deputy Sheriff Schweitzer requested the assistance of Detective Link, who purchased a device called the Shadow. (Tr. [49] at 69:20–23.) The Shadow is a handheld device about the size of a smartphone that allows the user to observe and locate wireless access points and station devices.

To observe access points and station devices,[2] the Shadow receives wireless radio signals within the immediate area. Access points and station devices emit these signals to facilitate Internet connections. An access point sends out a signal announcing its Internet connection, and a station device sends out a signal to locate available access points. The Shadow scans for these signals within range and displays the results on a touchscreen. The results show the detected access points and station devices and their relative signal strength. The Shadow can also display which station device is connected to a detected access point.

To locate access points and station devices, the Shadow displays the signal strength of a particular access point or station device selected by the user. This signal strength, labeled Received Signal Strength Indicator ("RSSI"), is displayed on the Shadow's screen in the range of -60 to 6. (Ex. D at 24.) As the Shadow gets physically closer to the selected access point or station device, the signal strength increases and the RSSI displays a higher number. Thus, the Shadow allows the user to locate a particular access point or station device by displaying the

[2] In this opinion, I will use the appropriate technical terms. But it can be a useful mental shorthand, in this case, to think of the station device as defendant's computer, and the access point as the hijacked router.

access point or station device's signal strength in real-time to the user.

On December 21, 2010, Detective Link observed a station device connected to an access point with an IP address subscribed to one of the six residences previously identified as using a P2P network to share child pornography files. The signal strength of the station device was weak near that residence, indicating that the station device was likely not inside the residence.

On January 18, 2011, Detective Link observed the now suspect station device connected to a different access point with an IP address subscribed to another residence previously identified as using a P2P network to share child pornography files. The signal strength of the station device was weak near that residence, too.

On January 24, 2011, Deputy Sheriff Schweitzer used investigative software to determine that a station device with a GUID known to have shared child pornography files was currently using an IP address subscribed to the J. residence, which was also one of the six residences previously identified as using a P2P network to share child pornography files. In addition, she determined the station device was actively uploading and downloading child pornography files at that time. (Tr. [49] at 40:10–17, 93:6–22.) She informed Detective Link of this active P2P network connection, and they met near the J. residence at approximately 6:40 p.m. Using the Shadow, Detective Link determined that the suspect device was connected to an access point with an IP address subscribed to the J. residence. Again, however, the Shadow showed that the signal strength of the suspect station device was weak near that residence.

To locate the suspect device, Detective Link walked south on a public sidewalk on the east side of defendant's residence at approximately 7:15 p.m. While standing on the sidewalk directly east of a window on the southeast corner of defendant's residence, Detective Link

observed "a spike in signal strength." (Schweitzer Aff. [42-1] at 19–20.) The spike correlated with RSSI numbers between -7 to -11. Detective Link testified at the suppression hearing that the spike was so significant that he immediately believed they had located the right residence. (Tr. [49] at 50:3–11.)

After the signal spike observation, Detective Link turned north on the public sidewalk towards the driveway of defendant's residence. When he reached the driveway, he turned west and walked up the driveway towards the residence. Near the residence's front entry, Detective Link observed the signal strength weaken with RSSI numbers between -45 and -39. Leaving the driveway, he walked across the front lawn of the residence and up to the southeast window. Here, he observed strong signals with RSSI numbers up to -5.

After gathering this data at defendant's residence, Detective Link and Deputy Sheriff Schweitzer returned to the J. residence and informed J. of their investigation. Using the Shadow in the J. residence, Detective Link and Deputy Sheriff Schweitzer confirmed the suspect station device was not located in the J. residence.

After leaving the J. residence, Detective Link and Deputy Sheriff Schweitzer returned to defendant's residence and initiated another Shadow use at approximately 8:01 p.m. Detective Link mirrored his 7:15 p.m. path with the Shadow. He walked down the public sidewalk and observed a similar spike in signal strength on the sidewalk directly facing the window on the residence's southeast corner. He also crossed defendant's front lawn and approached the southeast window. Here again, he observed strong signals with high RSSI numbers directly in front of it. (Tr. [49] at 53:11–54:3.)

III. Search Warrant Application and Execution

At this point in my recitation of the facts, it is important to underscore that Deputy Sheriff Schweitzer did not include all the information obtained during her investigation in the warrant affidavit. The suppression hearing provided a more complete explanation of the events leading up to the execution of the search warrant, and I have relied on that explanation to fully describe her investigation. But, because this case ultimately turns on the information in the warrant affidavit, I emphasis the distinction between the information described below, which is limited to the evidence included in the warrant affidavit, and the information provided before this point, which attempted to describe the relevant information known to the officers during their investigation.

Deputy Sheriff Schweitzer prepared a search warrant affidavit to search defendant's residence on February 15, 2011. She included six main pieces of evidence to support a finding of probable cause. First, Deputy Sheriff Schweitzer documented the ten IP addresses identified by Peer Spectre as using P2P networks to share child pornography files. She provided the dates of file transmission, the number of shared child pornography files, and confirmation of the file's content with the SHA-1 value or filename. Second, she provided the subscriber name and address of the ten IP addresses. She explained that the ten IP addresses were registered to six residences, including defendant's, in the Linwood School neighborhood. Third, she stated that the Internet connections of these ten IP addresses were accessible through unsecured wireless networks, which led her to believe that one individual was accessing all of them. Fourth, she stated that on January 26, 2011, she "noticed that seven of these IP addresses in this investigation were all using a consistent GUID" when connected to a P2P network. (Schweitzer Aff. [42-1] at 17.) The computer identified with this GUID was active between May 21, 2010, and January 25,

2011. The affidavit shows that none of the seven IP addresses associated with this GUID, however, was subscribed to defendant's residence. Fifth, she described Detective Link's elimination of two of the six residences as the location of the suspect station device. Sixth, she recounted Detective Link's use of the Shadow on January 24, 2011. Specifically, she detailed how Detective Link had eliminated the J. residence as the location of the suspect device (although she described this as having occurred before any Shadow use instead of in between the two uses). She also related Detective Link's observation of a spike in signal strength on the sidewalk across from defendant's southeast window and the weakened signal strength on defendant's driveway. Finally, she explained that the signal strength had been weak on the driveway because the residence and foliage had blocked it.

Deputy Sheriff Schweitzer did not distinguish between the 7:15 p.m. and 8:01 p.m. Shadow uses in the warrant affidavit. Instead, she described the Shadow use as a single event. In so doing, she intended to include only part of the data obtained with the Shadow. To this end, she excluded any reference to the front lawn portion of either Shadow use after describing the spike in signal strength on the sidewalk and the weakened signal strength on the driveway. (Tr. [49] at 68: 17–69:7, 115:25–117:14.) In addition to these verbal descriptions, Deputy Sheriff Schweitzer included an aerial photograph displaying the data obtained with the Shadow. Although it is not clear from the warrant affidavit itself, this aerial photograph plots the data obtained at 8:01 p.m. The fact that this aerial photograph correlates with the 8:01 p.m. Shadow use is apparent only when comparing the aerial photographs of the two Shadow uses and would not have been known to the judge issuing the search warrant.

On February 16, 2011, officers executed the search warrant and collected evidence of

child pornography crimes from defendant's computers. During the search, defendant also spoke with the officers and made incriminating statements. These two types of evidence are the subject of this motion to suppress [39].

DISCUSSION

I. Use of Shadow Device Generally

Defendant argues any use of the Shadow constituted a search under the Fourth Amendment and required a warrant. According to defendant, the Shadow monitored signals emitting from his station device, and thus it intruded upon a constitutionally protected privacy interest in those signals. Therefore, because Deputy Sheriff Schweitzer and Detective Link did not obtain a search warrant prior to using the Shadow, all evidence derived from the Shadow must be suppressed. The government responds that defendant lacked a reasonable expectation of privacy in the signals monitored by the Shadow. As a result, use of the Shadow did not constitute a search under the Fourth Amendment. For the following reasons, I agree with the government.

First, this case is very similar to those cases recognizing no reasonable expectation of privacy in stolen property. *See United States v. Caymen*, 404 F.3d 1196, 1200–01 (9th Cir. 2005) ("The Fourth Amendment does not protect a defendant from a warrantless search of property that he stole, because regardless of whether he expects to maintain privacy in the contents of the stolen property, such an expectation is not one that society is prepared to accept as reasonable.") (internal quotations and citation omitted). Here, the Shadow monitored the station device signals through the station device's connection to unsecured networks and could not have measured the station device signal strength without this connection (Tr. [49] at 126:23–127:7, 141:8–13.) Thus, when the Shadow was used to monitor the station device signals coming from defendant's

computer in his residence, the Shadow relied on the station device's unauthorized connection to his neighbor's unsecured network. Because the Shadow monitored the station device signals when the station device had no authorization to be on that network, defendant cannot claim a reasonable expectation of privacy in the signals. To put it more plainly: A defendant who connects to the Internet by hijacking his neighbor's wireless network does not have a privacy interest in the signals coming from his house that society is prepared to recognize as reasonable.

Second, defendant cannot assert a reasonable expectation of privacy "in information he voluntarily turn[ed] over to third parties." *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979). Through the station device, defendant voluntarily sent out a signal to amplify access point signals and attach to third parties' networks with his computer. Defendant cannot assert a reasonable expectation of privacy in signals he intentionally emitted to connect to unauthorized networks.

Third, from a practical standpoint, defendant's argument creates inconsistent expectations of privacy based only on the means by which an individual shares child pornography files over the Internet. On the one hand, this defendant would serendipitously receive Fourth Amendment protection because he hijacked another person's Internet connection to share child pornography files. On the other hand, another individual who uses his own Internet connection to share the same files lacks such protection, merely because the IP addresses would track back to his house. *See United States v. Borowy*, 595 F.3d 1045, 1047–48 (9th Cir. 2010); *United States v. Ganoe*, 538 F.3d 1117, 1127 (9th Cir. 2008). Both individuals are sharing child pornography files over the Internet starting from inside their home; the court should not recognize an expectation of privacy in one case simply because one individual uses a hijacked wireless signal. *See United*

States v. Skinner, 690 F.3d 772, 774 (6th Cir. 2012) ("When criminals use modern technological devices to carry out criminal acts and to reduce the possibility of detection, they can hardly complain when the police take advantage of the inherent characteristics of those very devices to catch them."). Consequently, I conclude defendant lacked a reasonable expectation of privacy in the station device signals and therefore cannot invoke the protection of the Fourth Amendment against the general use of the Shadow.

Defendant relies repeatedly on *Kyllo v. United States*, 533 U.S. 27, 34 (2001). In *Kyllo*, the Court held that when "the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant." 533 U.S. at 40. The principal distinction between this case and *Kyllo* is that in *Kyllo*, the heat signals were not being intentionally sent out into the world to connect publicly with others—let alone by an unauthorized boost from a neighbor's house.

The government sought to distinguish this case from *Kyllo* by putting on evidence that the public can purchase a device similar to the Shadow. (Tr. [49] at 132:24–133:9, 137:20–139:18.) It is often the case that an individual's subjective expectation of privacy is on a collision course with emerging technology. *See generally* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 Harv. L. Rev. 476 (2011). Some cases rely on the fact that technology is in general public use to determine that an individual's subjective expectation of privacy is not reasonable. I am not persuaded this continues to be a valid approach. But even under this theory, it is worth noting that there is a difference between a device that can be purchased by the public and "general public use." *Kyllo*, 533 U.S. at 40.

II. Trespass on Defendant's Property

In *United States v. Jones*, the Supreme Court held that a search under the Fourth Amendment occurs whenever "the [g]overnment obtains information by physically intruding on a constitutionally protected area." 132 S. Ct. 945, 950 n.3 (2012). The Ninth Circuit Court of Appeals has interpreted *Jones* as reaffirming the principle that "the home and its curtilage are sacrosanct" and that they are "areas expressly protected by the Fourth Amendment." *United States v. Duenas*, 691 F.3d 1070, 1080 (9th Cir. 2012). Accordingly, after *Jones*, there is no doubt that "[w]arrantless trespasses by the government into the home or its curtilage are Fourth Amendment searches." *United States v. Perea-Rey*, 680 F.3d 1179, 1185 (9th Cir. 2012) (citing *Jones*, 132 S. Ct. at 950 n.3).

Defendant contends Detective Link's actions fall squarely within the definition of a search under *Jones*. Detective Link trespassed on defendant's front lawn to obtain data with the Shadow regarding the location of the suspect station device. The government does not dispute that Detective Link trespassed on defendant's front lawn and offers no exigent circumstance for Detective Link's actions. (Resp. [42] at 15). I agree with defendant that Detective Link engaged in a warrantless search in violation of the Fourth Amendment when he physically trespassed on defendant's protected private property for the purpose of obtaining information.

Four non-exhaustive factors are examined to determine whether an area is part of a home's curtilage: "the proximity of the area claimed to be curtilage to the home, whether the area is included within an enclosure surrounding the home, the nature of the uses to which the area is put, and the steps taken by the resident to protect the area from observation by people passing by." *United States v. Dunn*, 480 U.S. 294, 307 (1987); *see Perea-Rey*, 680 F.3d at 1184–

85 (applying *Dunn* factors). "These factors do not yield a definite answer; rather they guide courts in determining whether the area is so intimately connected to the home that it should fall under the umbrella of the Fourth Amendment's protections." *United States v. Johnson*, 256 F.3d 895, 911 (9th Cir. 2001) (en banc) (Kozinski, J., concurring). Here, all four factors are met. The front lawn is next to the home and is included in the mixed enclosure of trees, shrubbery, and fence surrounding the home. The lawn appears well-kept with trimmed grass and trees, a garden, and a dog house. In addition to the enclosures, the lawn had at least two "Private Property/No Trespassing" signs. Because all four factors are satisfied, the front lawn is curtilage. Therefore, defendant's front lawn is afforded the same Fourth Amendment protection as the home, *see Duenas*, 691 F.3d at 1081, and Detective Link's trespass constituted an unlawful search under the Fourth Amendment, *see Perea-Rey*, 680 F.3d at 1186.

A. *Suppression*

Defendant moves to suppress the evidence obtained pursuant to the execution of the search warrant as a fruit of the unlawful search. "Because the curtilage is part of the home, searches and seizures in the curtilage without a warrant are . . . presumptively unreasonable." *Id.* at 1184. To avoid suppression, "[t]he government must prove the existence of an exception to the Fourth Amendment Warrant Requirement by a preponderance of the evidence." *United States v. Vasey*, 834 F.2d 782, 785 (9th Cir. 1987). Absent such an exception, the exclusionary rule requires suppression of all evidence derived from the unlawful search. *See United States v. Cervantes*, 678 F.3d 798, 807 (9th Cir. 2012).

1. Independent Source Doctrine

The government opposes suppression based on the independent source doctrine.

Specifically, the government argues that even if the evidence collected during the trespass was unlawfully obtained, all evidence obtained pursuant to the search warrant is admissible because the warrant affidavit omitted any reference to the evidence obtained during the trespass. Thus, the search warrant relied on only admissible evidence and is therefore an independent source.

The independent source doctrine is a well-established exception to the exclusionary rule. *See Murray v. United States*, 487 U.S. 533, 537 (1988). The Supreme Court has described two scenarios where the independent source doctrine applies. *Id.* The first scenario—the one applicable here—uses the doctrine in a "more general sense." *Id.* This approach "identifies *all* evidence acquired in a fashion untainted by the illegal evidence-gathering activity." *Id.* at 537–38. For example, "where an unlawful entry has given investigators knowledge of facts x and y, but fact z has been learned by other means, fact z can be said to be admissible because derived from an 'independent source.'" *Id.* at 538.

The "more general sense" independent source doctrine applies here because, if the evidence in the warrant affidavit was untainted by the trespass, the search warrant provided an independent means for acquiring evidence. In *Segura v. United States*, the Supreme Court applied the "more general" independent source doctrine. 468 U.S. 796, 813–16 (1984). In that case, law enforcement unlawfully entered defendant's apartment and discovered incriminating evidence in plain view. *Id.* at 800–01, 804. The following day, law enforcement obtained and executed a valid search warrant based on evidence wholly unrelated to the prior unlawful search. *Id.* at 801, 804. The Supreme Court upheld the admission of evidence seized pursuant to the valid search warrant because "none of the information on which the warrant was secured was derived from or related in any way to the initial entry into petitioners' apartment." *Id.* at 814.

Thus, the Court found "[t]he valid warrant search was a 'means sufficiently distinguishable' to purge the evidence of any 'taint' arising from the entry." *Id.* (quoting *Wong Sun v. United States*, 371 U.S. 471, 488 (1963)).

Here, the search warrant for defendant's residence did not provide a "means sufficiently distinguishable" from the unlawful search. In particular, the aerial photograph in the warrant affidavit was tainted by the unlawful search. As described above, this aerial photograph displayed the data obtained at 8:01 p.m. Because the information obtained during the trespassory portion of the 7:15 p.m. Shadow use prompted the 8:01 p.m. Shadow use, no data obtained during the 8:01 p.m. Shadow use should have been included in the warrant affidavit. The record reveals that the purpose of 8:01 p.m. Shadow use was to replicate the data obtained on defendant's property at 7:15 p.m. Significantly, Detective Link did not end his 8:01 p.m. Shadow use on the sidewalk or the driveway. Rather, he retraced his steps across defendant's front lawn, which implies that the strong signal data near the window was an important factor in his decision to return at 8:01 p.m. Indeed, Detective Link ended the 8:01 p.m. Shadow use within a few feet of defendant's window, precisely as he had done at 7:15 p.m.

Furthermore, although Detective Link testified that the first spike in signal strength at 7:15 p.m. made him believe that defendant's residence was the probable location of the suspect station device, the fact that he walked up to defendant's window a second time indicates that he did not actually believe he had sufficient reliable data to reach that conclusion prior to the trespass. An experienced officer would not take the dramatic and constitutionally improper action of trespass—well aware of the potential consequences for the case—without substantial doubts as to the adequacy of the evidence he already had at his disposal. What is more, the fact

that Detective Link and Deputy Sheriff Schweitzer agreed to remove all trespassory data from the warrant affidavit demonstrates that they were aware of the risk they were running.

Accordingly, based on my observations of the testimony and evidence, I conclude that the data observed during the trespass at 7:15 p.m. was a significant factor in motivating the 8:01 p.m. Shadow use. Therefore all data obtained during the 8:01 p.m. Shadow use was tainted. And because the aerial photograph included in the warrant affidavit visually displays data from the 8:01 p.m. use, it too should have been excluded from the warrant affidavit.

2. Probable Cause

Although the aerial photograph in the warrant affidavit was tainted by the unlawful search, suppression of all evidence does not necessarily follow. "[T]he mere inclusion of tainted evidence in an affidavit does not, by itself, taint the warrant or the evidence seized pursuant to the warrant." *United States v. Heckenkamp*, 482 F.3d 1142, 1149 (9th Cir. 2007) (quoting *United States v. Reed*, 15 F.3d 928, 933 (9th Cir. 1994)). To determine whether the search warrant and evidence obtained pursuant to the search warrant are tainted, "a reviewing court should excise the tainted evidence and determine whether the remaining untainted evidence would provide a neutral magistrate with probable cause to issue a warrant." *Id.* (quoting *Reed*, 15 F.3d at 933).

Probable cause is a flexible, common-sense standard. *Illinois v. Gates*, 462 U.S. 213, 238–39 (1983). A determination of probable cause is not an examination of each fact independent of the context in which the fact is found. Instead, facts are taken together in a totality of the circumstances analysis. *Id.* at 238. Probable cause exists where "there is a 'fair probability' that evidence of a crime will be found." *Chism v. Washington State*, 661 F.3d 380, 389 (9th Cir. 2011) (citing *Gates*, 462 U.S. at 238). Furthermore, "[i]n reviewing the validity of a

search warrant, a court is limited to the information and circumstances contained within the four corners of the underlying affidavit." *United States v. Stanert*, 762 F.2d 775, 778 (9th Cir. 1985). Therefore, to determine whether the evidence obtained pursuant to the search warrant is admissible here, I must excise the tainted evidence and ask whether there was still sufficient evidence in the warrant affidavit to create a "fair probability" that evidence of child pornography crimes would be found in defendant's residence.

The evidence in the warrant affidavit began with information regarding the ten IP addresses that had shared child pornography files through P2P networks. A unique IP address is assigned by the ISP to each device accessing the Internet connection provided by the ISP to the subscriber. The IP address assigned to a device identifies the subscriber of that Internet connection. In this sense, an IP address is similar to a land-line telephone number because the telephone number assigned by the telephone provider can identify the subscriber of that telephone service. An IP address differs from a land-line telephone number, however, in that multiple IP addresses can be registered to one subscriber. In particular, when an Internet subscriber allows his Internet connection to be accessible through an unsecured wireless network, any device within that network's signal range can access that network and devices accessing that unsecured wireless network will be assigned an IP address by the ISP identifying the subscriber. Thus, a subscriber can have multiple IP addresses registered to him due to authorized and unauthorized devices accessing his unsecured wireless network.

Here, Deputy Sheriff Schweitzer determined ten IP addresses were registered to six residences in one neighborhood, including defendant's residence. But, because the Internet connections were accessible through unsecured wireless networks, any device in any residence,

business, or even vehicle within signal range could have been accessing the six residences' Internet connections. (Tr. [49] at 91:20–92:19.) Thus, the IP address information restricted the general area in which the suspect station device could be located, but this information alone could not possibly identify or eliminate any specific location within that area. The IP addresses provided no reason to believe any one of the six subscriber residences—as opposed to any other location in the neighborhood—was the probable location of the suspect device, and no reason to single out defendant's home. For the same reasons, the elimination of three out of the six subscriber residences did very little to narrow the scope of the investigation. There was nothing about the elimination of those three residences that identified one of the remaining three subscriber residences—as opposed to any other home or car in the area—as the probable location of the suspect device. Therefore, prior to the 7:15 p.m. Shadow use, the elimination of three residences did not create a "fair probability" that evidence of child pornography crimes would be found in any specific location, since there were many homes, businesses, and vehicles in which the suspect device might have been operating.

The warrant affidavit also included some of the evidence obtained during the 7:15 p.m. Shadow use near defendant's residence, but this evidence also fell short of the "fair probability" standard. Without the tainted aerial photograph displaying the RSSI data, and without the more complete explanation of the Shadow device provided at the suppression hearing, all that remained in the warrant affidavit was Deputy Sheriff Schweitzer's testimony that she and Detective Link observed a spike in signal strength when standing on the sidewalk facing the window on the southeast corner of defendant's residence. (Schweitzer Aff. [42-1] at 19–20.) In contrast to the thorough explanations provided for the other relevant technologies, the warrant

affidavit provided only three short paragraphs to explain how this new Shadow technology worked. This limited description of the Shadow technology provided little context to understand the spike in signal strength and its relation to other Shadow data obtained in the neighborhood.

For example, no information was provided on the relationship between signal strength and actual distance from the source of the signal. Thus, as far as the issuing judge knew the spike in signal strength could have meant the Shadow was two feet or two blocks away from the suspect device. Additionally, no information was provided to understand the magnitude or significance of the spike. From the suppression hearing, I learned that the Shadow RSSI number range is from -60 to 6. Presumably, a RSSI jump from -60 to -40 would be considered a spike in signal strength, but that kind of spike would not tell the officers much about the location of the suspect device. In sum, a spike in signal strength, without more, is open to interpretation, especially when the technology is so unfamiliar and complex.

Perhaps some of this missing information in the warrant affidavit could be attributed to the fact that this investigation was the first time the Clackamas County Sheriff's Office used the Shadow. Nonetheless, an officer must provide the issuing judge with sufficient information to understand the technology at issue. And although the suppression hearing more fully explained the Shadow technology, this information cannot be used retrospectively to evaluate the legality of the warrant affidavit. *See Stanert*, 762 F.2d at 778.

Consequently, an ambiguous spike coupled with a limited description of the Shadow technology did not establish a "fair probability" that evidence of child pornography crimes would be found in defendant's residence.

The GUID confirmation also failed to support a finding of probable cause to search

defendant's residence. While the consistent GUID confirmed Deputy Sheriff Schweitzer's belief that one peer with one computer was accessing multiple Internet connections, none of the IP addresses associated with this GUID was subscribed to defendant's residence. Therefore, the GUID confirmation actually suggested that defendant's residence might not have been the location of the suspect station device. This, too, undermined a finding of probable cause.

Earlier in this opinion, I reasoned that perverse incentives would result from a finding that this defendant had a reasonable expectation of privacy in his wireless radio signals simply because he stole an Internet connection. It might be said that this point in the analysis raises a similar concern about perverse incentives. Namely, this defendant who hides behind several IP addresses to share child pornography files can thwart an officer's effort to establish probable cause, while another individual who used his own IP address to share the same files would not be able to do so.

One distinction to be made is that two very different concepts, raising different underlying principles, are at play: a reasonable expectation of privacy and probable cause. Another explanation for my finding is that these facts are distinguishable from other investigations of child pornography file sharing over P2P networks. As a general matter, I recognize "the utility of using IP address information to investigate child pornography offenders." *Chism*, 661 F.3d at 390; *see also United States v. Craighead*, 539 F.3d 1073, 1080–82 (9th Cir. 2008) (holding that probable cause existed where the IP address from which child pornographic images were shared was traced to the defendant); *United States v. Hay*, 231 F.3d 630, 634–35 (9th Cir.2000) (holding that an affidavit demonstrated probable cause where the agent carefully detailed how the IP address associated with the child pornographic images was

connected to the defendant). But, unlike the investigations in *Craighead* and *Hay* where the warrant affidavit traced one or two IP addresses back to one defendant, Deputy Sheriff Schweitzer here identified ten IP addresses subscribed to six residences all with unsecured networks. *See Craighead*, 539 F.3d at 1077 (one IP address); *Hay*, 231 F.3d at 632 (two IP addresses subscribed to one apartment). On these facts, the straightforward chain of probable cause analysis in *Craighead* or *Hay* became more complex and uncertain. And this is clear from the warrant affidavit, where the affiant herself did not think that evidence of an IP address known to have shared child pornography files amounted to probable cause to search any one of the six houses, without more.

Therefore, considering the totality of the circumstances here, the information in the warrant affidavit did not create a fair probability that evidence of child pornography crimes would be found in defendant's residence. Accordingly, all evidence obtained pursuant to the execution of the search warrant must be suppressed.

This is not to say that officers cannot obtain search warrants in these types of multiple-location investigations. They will be greatly assisted in doing so if they do not trespass on a suspect's property. In addition, if they correctly include a more complete set of data (here, the correct photograph), and a more thorough explanation of the investigation and the relevant technology, it would allow the court to better assess probable cause. Significantly for my analysis, that was not the case here.

3. Good Faith Exception

"The good faith exception does not apply where a search warrant is issued on the basis of

evidence obtained as the result of an illegal search." *United States v. Wanless*, 882 F.2d 1459, 1466 (9th Cir. 1989). As the Ninth Circuit has explained when applying the good faith exception, if a search warrant is issued partially on the basis of evidence obtained from an unlawful search, the search conducted pursuant to that warrant is valid "only if the legally obtained evidence, standing alone, was sufficient to establish probable cause." *Id.* at 1467. Here, I have found the lawfully obtained evidence in the warrant affidavit was insufficient. Therefore, the government cannot rely on the good faith exception.

CONCLUSION

For the foregoing reasons, defendant's motion to suppress [39] is GRANTED. The evidence obtained pursuant to the execution of the search warrant and defendant's statements made during its execution are suppressed.

IT IS SO ORDERED.

DATED this 28th day of November, 2012.

/s/ Michael W. Mosman
MICHAEL W. MOSMAN
United States District Judge